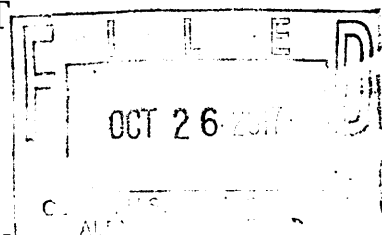


UNDER SEAL UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia



In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
Information associated with Facebook user IDs
"Ben.Manlapaz.JBMFinancialGroup" and
"100008768172560," stored at premises controlled by
Facebook, Inc.

Case No. 17-SW-708

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
See Attachment A.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):
See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 371, 1349, 1341,	Conspiracy, mail fraud, wire fraud, money laundering, identity theft and aiding and
1343, 1956, 1957, 1028(a)(7),	assisting in the preparation of false tax returns
26 U.S.C. § 7206(2)	

The application is based on these facts:
See attached affidavit.

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

AUSA Katherine L. Wong

Applicant's signature

Michael Wheeler, Special Agent, IRS-CI

Printed name and title

Sworn to before me and signed in my presence.

Date: 10/26/2017

City and state: Alexandria, VA

/s/ **JFA**
John F. Anderson
United States Magistrate Judge
Judge's signature

The Honorable John F. Anderson, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF)
INFORMATION ASSOCIATED WITH)
FACEBOOK USER IDs:)

Case No. 17-SW-~~709~~ 708

“Ben.Manlapaz.JBMFinancialGroup”, and)
“100008768172560”.)

UNDER SEAL

STORED AT PREMISES CONTROLLED)
BY FACEBOOK INC.)

ATTACHMENT A
Places to Be Searched

This warrant applies to any and all information associated with the Facebook IDs
“Ben.Manlapaz.JBMFinancialGroup” and “100008768172560,” that are stored at a premises
owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in
Menlo Park, California.

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF)
INFORMATION ASSOCIATED WITH)
FACEBOOK USER IDs:)

Case No. 17-SW-~~709~~ 708

"Ben.Manlapaz.JBMFinancialGroup", and)
"100008768172560".)

UNDER SEAL

)
STORED AT PREMISES CONTROLLED)
BY FACEBOOK INC.)

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by FACEBOOK, Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A for the period of 2008 to present:

- (a) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;
- (b) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;
- (c) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which

- the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;
- (d) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;
 - (e) All "check ins" and other location information;
 - (f) All IP logs, including all records of the IP addresses that logged into the account;
 - (g) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";
 - (h) All information about the Facebook pages that the account is or was a "fan" of;
 - (i) All past and present lists of friends created by the account;
 - (j) All records of Facebook searches performed by the account;
 - (k) All information about the user's access and use of Facebook Marketplace;
 - (l) The types of service utilized by the user;
 - (m) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
 - (n) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

- (o) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.
- (p) The files, contents and metadata associated with the accounts related to Facebook services such as Facebook Likes, Facebook search history, Facebook bookmarks, Facebook drive files, Facebook purchases, Facebook Sites, Facebook notifications, Facebook uploads and activity (including but not limited to the user's profile, posts, chats, messages and emails, comments), Facebook followers.
- (q) All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number), screen names, Facebook security questions and answers, contact email addresses, websites and other personal identifiers;
- (r) Records or information (cookie data), to include unique identifying information, of all devices that have accessed target accounts

II. Information to be Seized by the Government

A. All information described in Section I above, including but not limited to correspondence, records, documents, photographs, videos, electronic mail, chat logs, and electronic messages, that constitutes evidence, contraband, and fruits of violations of the

preparation of false and fraudulent tax returns (26 U.S.C. § 7206(2)), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), conspiracy to defraud the United States (18 U.S.C. §§ 371, 1349), money laundering (18 U.S.C. §§ 1956, 1957), and identity theft (18 U.S.C. § 1028(a)(7)), including, for each account or identifier listed on Attachment A, information pertaining to the following matters for the period of 2008 through present:

1. Any records, documents, communications or other materials related to the preparation of federal income tax returns or state tax returns;
2. Any records, documents, communications or other materials related to communications with the U.S. Internal Revenue Service or state tax authorities;
3. Any records, documents, communications or other materials related to advertising the services offered by JBM, including but limited to those related to tax preparation, ITINs, or responding to IRS letters/audits;
4. Any records, documents, communications or other materials related to the identities, roles, and relationships of employees in JBM, including who had a management and/or supervisory role;
5. Any records, documents, communications or other materials related to the IRS criminal investigation, including the search in 2013;
6. Any records, documents, communications or other materials related to the training, certifications or qualifications of Ben Manlapaz or others employees of JBM to prepare tax returns;
7. Any records, documents, communications or other materials related to identifying clients of JBM;

8. Any records, documents, communications or other materials related to the disposition of proceeds earned by Ben Manlapaz and/or JBM, including the manner and means for paying employees in the Philippines;
9. Any records, documents, communications or other materials related to the use of cash or the sending of JBM proceeds outside of the United States;
10. Any records, documents, communications or other materials related to books and records of JBM, including any client lists;
11. Any records, documents, communications or other materials related to the JBM office in the Philippines and its role in preparing materials submitted to the IRS or state tax authorities;
12. Any records, documents, communications or other evidence showing who used, owned, or controlled the accounts or identifiers listed on Attachment A;
13. Any records, documents, communications or other evidence of the times the accounts or identifiers listed on Attachment A were used, updated or revised;
14. Any records, documents, communications or other evidence of passwords or encryption keys and other access information that may be necessary to access the accounts or identifiers listed on Attachment A and other associated accounts.

UNDER SEAL

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF)
INFORMATION ASSOCIATED WITH)
FACEBOOK USER IDs:)

Case No. 17-SW-~~709~~ 708

“Ben.Manlapaz.JBMFinancialGroup”, and)
“100008768172560”.)

UNDER SEAL

STORED AT PREMISES CONTROLLED)
BY FACEBOOK INC.)

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT

I, Michael J. Wheeler, being duly sworn, depose and declare the following:

INTRODUCTION

1. I make this affidavit in support of an application for a search warrant for information associated with Facebook user IDs “Ben.Manlapaz.JBMFinancialGroup” and “100008768172560” (hereinafter, “SUBJECT FACEBOOK ACCOUNTS”) that are stored at premises owned, maintained, controlled, or operated by Facebook Inc. (hereinafter, “Facebook”), a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the SUBJECT FACEBOOK ACCOUNTS with the identifiers listed in Attachment A.

2. I am a Special Agent with Internal Revenue Service Criminal Investigation (hereinafter, “IRS-CI”) and have been so employed since July 2012. Prior to July 2012, I was

employed by an international accounting firm for approximately three years. I am a Certified Public Accountant, a Certified Government Financial Manager, and a Certified Fraud Examiner. I am also certified in Information Security Fundamentals. My training has included financial investigative techniques, accounting, tax, criminal investigation techniques, criminal law and search warrants. As an IRS-CI Special Agent, I investigate potential violations of the Internal Revenue Code (Title 26), the Money Laundering Control Act (Title 18) and the Bank Secrecy Act (Title 31). By virtue of my training and experience, I am familiar with investigations involving allegations and violations related to the preparation of false and fraudulent tax returns (26 U.S.C. § 7206(2)), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), conspiracy to defraud the United States (18 U.S.C. § 371), money laundering (18 U.S.C. §§ 1956, 1957), identity theft (18 U.S.C. § 1028(a)(7)) and other white collar and financial violations.

3. Based on the facts set forth herein, I submit there is probable cause to believe that Jose Benjamin Manlapaz (hereinafter, "Manlapaz"), owner of JBM Financial Services, which recently also went by the name JBM Financial Group, committed the following offenses together with others known and unknown to the investigation: aiding or assisting in the preparation of fraudulent tax returns, in violation of 26 USC § 7206(2), conspiracy to defraud the United States, in violation of 18 USC §§ 371 and 1349, mail fraud, in violation of 18 USC § 1341, wire fraud, in violation of 18 USC § 1343, identity theft, in violation of 18 USC § 1028(a)(7), and money laundering, in violation of 18 USC §§ 1956, 1957. Based on the information set forth herein, I submit there is probable cause to believe that evidence, fruits and instrumentalities of these offenses will be found in the above-described SUBJECT FACEBOOK ACCOUNTS.

4. This Affidavit is based upon information gained by me from multiple sources; including but not limited to, recorded conversation and correspondence obtained during an

undercover investigation, surveillance, a review of Internal Revenue Service (hereinafter, "IRS") databases, a review of Federal income tax return information, witness interviews, a review of email account records obtained via search warrant in 2013 issued by the Honorable Ivan D. Davis (13-SW-671), a review of records obtained from a search of JBM's offices in May 2013 and again in May 2017, consent searches of former employee's email accounts that were active at the time of the second search in May 2017, a review of records obtained from a search of Manlapaz's residence in May 2017, information received from other IRS personnel, and knowledge gained from my training and experience. Because this Affidavit is written and offered for the limited purpose of establishing probable cause for the issuance of search warrants, it does not contain all of the information that the Government possesses relative to this investigation.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States ...that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

6. The investigation has revealed that Manlapaz operated his tax preparation business in the Eastern District of Virginia. Manlapaz also lived in the Eastern District of Virginia during the relevant time period.

PROBABLE CAUSE

7. In or around 2012, the IRS identified tax return preparer Manlapaz and his business, JBM Financial Services/Group (hereinafter "JBM"), based on data analysis as having potentially fraudulent tax preparation activity. At that time, JBM was located at 6201 Leesburg

Pike Suite 218, in Falls Church, Virginia. By the time of the 2016 tax preparation season, it had moved to Suite 405 at the same address.

8. On or about March 21, 2013, an Undercover Agent (hereinafter, "UCA") walked into JBM at 6201 Leesburg Pike Suite 218, Falls Church, Virginia 22044 in an attempt to have an income tax return prepared by Manlapaz.

9. Upon entering Suite 218, the UCA was greeted by a female employee. This female employee conducted intake procedures and the UCA provided their undercover personal information and a 2012 Form W-2 that had been created by IRS-CI. After providing the required information, the UCA waited in the waiting area until it was his/her turn to meet with Manlapaz in his back office.

10. Manlapaz eventually called the UCA into his office and explained that the UCA would owe approximately \$500 if Manlapaz prepared the Federal income tax return correctly. Manlapaz asked the UCA if he/she needed money and then offered to provide the UCA with a tax refund of approximately \$1,900 by placing a fraudulent education credit on their Federal income tax return.

11. Manlapaz further explained what an IRS audit was and what the UCA should do if his/her Federal income tax return was audited. Manlapaz directed the UCA to bring any IRS audit correspondence to him and stated that he would respond to the audit on the UCA's behalf.

12. If Manlapaz had prepared the 2012 Federal income tax return correctly, the resulting tax due and owing would have been approximately \$520. Manlapaz instead placed \$4,000 of fraudulent qualified education expenses on a Form 8863, Education Credits, for the UCA, which resulted in a \$1,000 refundable American opportunity credit and a \$1,500 nonrefundable education credit. These credits combined to provide the UCA with a Federal tax

refund of \$1,981. The Form 8863 that Manlapaz prepared fraudulently indicates that the UCA incurred qualified education expenses with Stratford University at 7777 Leesburg Pike, Falls Church, Virginia 22043. The UCA did not provide Manlapaz or JBM with information or documentation for these fraudulent education credits.

13. The UCA paid a second female JBM employee \$195 in cash and received an invoice stamped "PAID" in return. This second female employee also provided the UCA with a printed copy of his/her Federal and State income tax returns and informed the UCA that JBM would send copies of the tax returns to the residential address the UCA provided earlier.

14. Manlapaz is listed as the paid preparer on the UCA's 2012 Federal tax return. Manlapaz is also listed as a third party designee, which authorized him to discuss the tax return with the IRS.

15. On or about May 15, 2013 law enforcement conducted a search warrant of JBM's offices (hereinafter, "2013 search"), seizing client files and other documents related to the preparation of tax returns. Law enforcement also seized various electronic files containing Manlapaz's work-related emails for the period of at least 2008 through May 2013.

16. During subsequent interviews of former JBM employees and based on a review of the May 2013 search warrant materials, law enforcement learned that Manlapaz taught JBM employees how to prepare fraudulent tax returns claiming false items such as education credits, childcare expenses, and false Schedule Cs (businesses). For example, former employee G.E. explained how s/he was trained by other JBM employees to use a list of educational institutions that JBM created and maintained, along with an online mapping tool to locate an educational institution close to a client's address. JBM employees were then instructed to add this educational institution to the client's tax return data, regardless of whether or not the client

actually attended a qualifying educational institution or had provided any documentation about educational expenses during their intake interview. G.E. also explained how s/he was taught to claim certain amounts of education expenses. Based on my knowledge, training, and experience, I know that the amounts of education expenses that G.E. was trained to claim has the effect of largely maximizing the benefit of the education tax credit.

17. During subsequent interviews of former JBM employees and based on a review of the May 2013 search warrant materials, law enforcement learned that Manlapaz and JBM had a satellite office in the Philippines managed by Diana Dela Cruz (hereinafter, "Dela Cruz") under the direction of Manlapaz. The primary method of communication between Dela Cruz, Manlapaz and other JBM employees was by email. Dela Cruz used the "dianadelacruz2011@gmail.com" account.

18. If a JBM client was audited and asked for supporting documentation by the IRS, my investigation has revealed that employees were taught to email Dela Cruz in the Philippines. In many instances, the IRS audit letters informed the client that the IRS did not have any record of the purported expenses claimed on the return, and was requesting documentation from the taxpayer. For example, former employee E.Q. explained how s/he would assist clients who would come into JBM with IRS audit letters. E.Q., using email account "ericaq0894@gmail.com", would email Dela Cruz at "dianadelacruz2011@gmail.com" with the client name, the educational institution listed on the client's tax return that was under audit, the tax year, and the educational expense amount. In response, Dela Cruz would email E.Q. a false and fraudulent Form 1098-T that was supposed to contain the information that E.Q. previously requested. E.Q. noted how Manlapaz instructed him/her to pay close attention as to how the Forms 1098-T produced by Dela Cruz appeared and ensure that the Forms 1098-T looked as

close to an authentic document as possible. In other instances, E.Q. and other employees would email Dela Cruz to request documents to substantiate other fraudulent items on client returns, such as medical expenses or childcare expenses. These fraudulent documents were often created from scanned copies of real, genuine receipts that JBM obtained from other clients and would then send to Dela Cruz by scanning the originals.

19. On August 9, 2013, E.Q. sent law enforcement an email from "ericaq0894@gmail.com" that showed a Form 1098-T for taxpayer Samuel Banya sent from "dianadelacruz2011@gmail.com" to "ericaq0894@gmail.com" on May 13, 2013. The email was signed by Dela Cruz. The Form 1098-T showed \$3,116 in qualified education expenses from Northern Virginia Community College for Samuel Banya for tax year 2011. Per IRS data, Jose Benjamin Manlapaz and JBM Financial Services prepared a tax year 2011 tax return for Samuel Banya that claimed \$2,500 in education credits and a tax refund of \$3,757. IRS data show no Form 1098-T on file for this tax return, which means that no educational institution reported any such qualified education expenses for this taxpayer. According to records obtained from Northern Virginia Community College (hereinafter, "NVCC"), Samuel Banya has never completed any credit hours with them or paid them any qualified education expenses.

20. According to interviews of JBM employees who worked there after the 2013 search and clients who had tax returns prepared after the 2013 search, JBM continued to prepare false and fraudulent tax returns after the 2013 search. In order to conceal the preparation of tax returns, Manlapaz no longer lists himself or "JBM" in the paid preparer section of the tax return and files the majority of tax returns by mailing them to the IRS. Manlapaz also directed JBM employees to obtain electronic filing identification numbers, but not list their association with JBM on the necessary IRS applications.

21. Records seized during the 2017 search show that Manlapaz was trying to grow JBM, with a goal of 4,000 clients for the 2017 tax year. JBM records show that JBM prepared thousands of returns for tax years 2013, 2014, 2015 and 2016. Manlapaz oversaw and directed the procedures used to prepare these returns, which included him signing off on tax returns before they were filed. Former employees have also stated that the price charged to JBM clients generally reflected the number of false items placed on the return, and thus the refund amount. Based on a review of records from the search in May 2017 (hereinafter, "2017 search"), I know some clients were charged between \$300 and \$1,000 for JBM to prepare their return. High fees is often a characteristic of tax preparation services that add false items to generate larger, fraudulent refunds.

22. One of the other services that JBM offered was filing for Individual Tax Identification Numbers (hereinafter, "ITINs") with the IRS. Manlapaz encouraged clients to obtain ITINs for friends and relatives located overseas, who would then be fraudulently added to the clients' tax return as dependents. These friends or relatives should not have been added to the return, because they did not live with the client, were generally not even in the United States, and sometimes even lacked a qualifying familial relationship with the taxpayer. Former JBM employees described how they were instructed to falsify the ITIN applications to make it appear that the individual lived in the United States, and sometimes list a false relationship to the taxpayer on the tax return.

23. Interviews of JBM employees and clients have revealed that Manlapaz and JBM caused the preparation of additional false tax returns for tax years 2014 through 2017, using largely the same methodology and techniques employed before the 2013 search. After the 2017 search warrant, law enforcement has interviewed multiple former JBM employees who were

recently employed by Manlapaz. These individuals described a tax preparation business that was still permeated with fraud. For example, one former JBM employee noted that s/he was tasked with correcting client intake interview worksheets after the tax returns had been prepared. This individual was instructed to make sure the client interview worksheets supported what was claimed on the tax returns and if they did not, to add items such as education expenses and childcare expenses to the worksheet in order for the documents to match up. This after-the-fact alteration would thus give the appearance to anyone reviewing the paperwork that the client provided the information to support the false and fraudulent credit and deductions listed on their tax returns. When asked how many client interview worksheets s/he had to correct, the former JBM employee stated that every worksheet s/he reviewed required additions. Law enforcement has reviewed a number of client interview worksheets seized during the 2017 JBM search warrant and noted that many of them have different sets of handwriting and, in some cases, different colored ink. The items written with different handwriting and/or ink are often items that would support particular credits and/or deductions on the clients' tax returns.

24. Several clients of JBM filed complaints with the IRS as recently as 2016 and 2017, alleging that JBM prepared tax returns that included false and fraudulent items, including education credits, without their knowledge or permission. The investigation has also revealed that JBM has continued to prepare responses to IRS audit letters (hereinafter "IRS letters"). To prepare these responses, employees have continued to contact Dela Cruz in the Philippines and request fraudulent documentation. This documentation is then submitted to the IRS.

25. The investigation, including a review of bank accounts in the name of JBM and Manlapaz, shows that some of the proceeds from JBM were sent outside the United States, to Dela Cruz in the Philippines. E.C., a friend of Manlapaz and client of JBM, also stated that he

agreed to send cash given to him by Manlapaz to the Philippines after the 2013 search. On two occasions, E.C. attempted to send tens of thousands of dollars in cash to the Philippines. At the time, the only apparent source of income for Manlapaz was JBM. Since then, the investigation has revealed that Manlapaz generally kept his cash separate from his wife, who is a doctor with her own medical practice.

FACEBOOK USER ID Ben.Manlapaz.JBMFinancialGroup

26. I have reviewed the publicly available Facebook account associated with User ID Ben.Manlapaz.JBMFinancialGroup. The account indicates the accountholder is “very responsive” to messages and typically replies within a day. There is also a link on the page that says “send message”. Clicking on this link brings up a Facebook message directed to JBM Financial Group and encourages the user to “type a message”.

27. The Ben.Manlapaz.JBMFinancialGroup account has pictures of Manlapaz and employees of JBM; it also was used to advertise JBM’s services. For example:

- A. On or about April 25, 2017 a photo was posted stating the JBM office was open for essential services only, to include extensions on IRS letters and notices and intake interviews on new IRS letters and files. A Spanish language version of what appears to be the same information was posted on or about the same day.
- B. On or about February 20, 2016 a photo was posted listing JBM’s services, to include tax preparation, IRS audit resolution, applications for ITINs, tax amendments, “recover tax paid from frivolous tax return preparers”, Philippines passport services, Philippines business registrations, and Philippines business audits. The same photo indicates that Manlapaz, Dela Cruz, and Arlene Camacho Pascual should be asked about the Philippines-based services.

- C. On or about January 6, 2016 a photo was posted that explains to clients what they should bring to the tax interview, to include wage statements, child care expenses, charitable contributions, education and tuition expenses to include Forms 1098-T, and self-employment business receipts.
- D. On or about January 6, 2016 a photo was posted with general JBM contact and location information, including the phone number for Dela Cruz.
- E. On or about January 1, 2016 a photo was posted that is a personal letter from Manlapaz to his clients. This letter states that Manlapaz has hired competent individuals for the coming tax season and that he has trained them and will continue to train them. Manlapaz also states that he is consistently learning about tax laws, going to tax forums, and understanding IRS positions related to tax law. Manlapaz says that he will exhaust all efforts to resolve any IRS issues the clients may have and he closes by encouraging his clients to refer their family and friends since JBM is a referral only company.
- F. On or about September 6, 2015 the account posted a link to a New York Times article titled "Hacking of Tax Returns More Extensive Than First Reported, I.R.S. Says" with the caption, "IF YOU HAVE BEEN WRITTEN A LETTER, WE NEED TO ANSWER IMMEDIATELY ... come to the office and I will file a report and protect your identity."
- G. On or about February 27, 2015 the account posted information titled "What you need to know about the Child Tax Credit". This includes information about qualifications and certain tests that are applied regarding age, relationship, support, dependency, citizenship, residence, and others.

28. The SUBJECT FACEBOOK ACCOUNT also has correspondence with other Facebook Accounts, including a Facebook account in the name of Rosie Statler (hereinafter, "Statler"). The account 100008768172560, a personal account registered to "Ben Manlapaz," is "friends" with the Statler account, which lists Statler as living in Winchester, Virginia. According to IRS records, Rosie Statler of Winchester, Virginia, filed her tax year 2014 and 2015 tax returns on or about November 19, 2016. Her 2014 tax return claimed a Schedule C self-employment business loss of more than \$4,000; Statler received tax refunds of more than \$2,000 for both tax years. There is no paid preparer listed on these tax returns. Based on interviews of JBM clients and former JBM employees I know that Manlapaz prepared tax returns from at least tax year 2013 through at least tax year 2016 without filling out the paid preparer section. I also know from former JBM employees that Manlapaz would sometimes direct employees to create a fraudulent Schedule C in order to increase a client's tax refund.

FACEBOOK USER ID "100008768172560"

29. According to Facebook records obtained via a § 2703(d) order signed by the Honorable Michael S. Nachmanoff (17-ec-930) for User ID 100008768172560 and Ben.Manlapaz.JBMFinancialGroup, Facebook user ID "100008768172560" belongs to "Ben Manlapaz". I have reviewed the message headers related to the "100008768172560" Facebook account obtained via the § 2703(d) order. The headers show the message participants as well as the date and time stamps of the messages. I have also reviewed the publicly available Facebook page information. A review of this data shows the following:

A. Photos of Manlapaz and former JBM employees are posted to the account.

Photos of information related to JBM's tax preparation and other services are also posted to the account.

- B. The account lists Manlapaz as a “Tax Audit and Compliance Manager at JBM Financial Group” from 1998 to present. The work description for this position states, “I respond to IRS letters and audits. I also make sure that returns are compliant with IRS Tax Laws and Revenue Codes. Since the Internal Revenue Code is so complex, the need for proper interpretation is of paramount importance to our clients, both business and personal. When it comes to the IRS, our policy is simple: We offer simple solutions to complex problems. This is of outmost importance to me now more than ever before. Come and let’s talk about your tax benefit.”
- C. On or about April 24, 2017, the 100008768172560 account authored a message to Daniela Mochorro, who responded on or about May 23, 2017. At the time of these messages, Daniela Mochorro was employed by JBM and MANLAPAZ.
- D. Between October 2016 and May 2017, the 100008768172560 account authored or received messages from an account in the name of Yuyu Aragon. Based on interviews with former JBM employees, I know that Yuyu Aragon was also employed by JBM for a period of time.
- E. From June 2015 through May 2017, the 100008768172560 account corresponded with an account in the name of Eve Smith (hereinafter, “Smith”) who was listed as living in Manassas, Virginia. According to IRS records, Eve Smith of Manassas, Virginia, had her tax year 2010, 2011, and 2012 tax returns prepared by Manlapaz and JBM. Smith’s tax year 2013 and 2014 tax returns do not list any paid return preparer. Based on interviews of JBM clients and former JBM employees I know that Manlapaz prepared tax returns from at least

tax year 2013 through at least tax year 2016 without filling out the paid preparer section. Smith's tax year 2010 through 2014 tax returns claim at least \$1,000 in education credits each year, which was a credit that Manlapaz routinely directed employees to add to client returns in order to fraudulently increase their refund.

- F. From November 2016 through May 2017, the 100008768172560 account corresponded with an account in the name of Khoeun Ly (hereinafter, "Ly"). The 100008768172560 account is friends with the Ly account. Based on publicly available Facebook data, the person controlling the Ly account has repeatedly been in and around the Charlotte, North Carolina area. According to IRS records, Khoeun Ly of Charlotte, North Carolina had their tax year 2010, 2011, and 2012 tax returns prepared by JBM. Ly's tax year 2013 through 2016 tax returns do not list a paid return preparer. Ly's tax year 2010 through 2016 tax returns all claim at least \$1,000 in education credits each year.
- G. On or about July 22, 2016, on or about February 8, 2017, and on or about May 23, 2017 the account corresponded with an account in the name of Grace Kimball (hereinafter, "Kimball"). According to Facebook records, Kimball lives in Northern Virginia and works at Sunrise Senior Living. According to IRS records, Grace Kimball of Northern Virginia who works at Sunrise Senior Living had her tax year 2010, 2011, and 2012 tax returns prepared by JBM and Manlapaz. Kimball's tax year 2010, 2011, and 2012 tax returns claim at least \$1,000 in education credit each year.

TECHNICAL BACKGROUND

30. Based on my training and experience, I know that businesses often use Facebook to advertise their services and promote relationships with existing clients/employees. In this case, I believe the SUBJECT FACEBOOK ACCOUNTS were used by Manlapaz for those purposes and to correspond with employees. For example, after "friending" a person on Facebook, that friend will generally receive updates and posts. In this case, some of the posts include advertisements of JBM's services.

31. I have consulted with an IRS-CI special agent who is assigned to the Technology Operations and Investigative Services Division with IRS-CI's Washington, DC Field Office and has training, experience, and expertise in computers. That Special Agent confirmed to me that the technical background contained in this section of my affidavit is accurate.

32. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

33. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

34. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

35. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

36. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user

and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

37. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to “tag” (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook’s purposes, the photos and videos associated with a user’s account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

38. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient’s “Inbox” on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

39. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

40. Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through

the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

41. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (hereinafter, “apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

42. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings; rejected “Friend” requests; comments; tags; and information about the user’s access and use of Facebook applications.

43. Facebook also retains Internet Protocol (hereinafter, “IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

44. Social networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the

service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

45. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's "Neoprint," IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used.

46. For example, as described herein, Facebook logs the IP addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally,

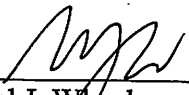
Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

47. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

CONCLUSION


48. Based on my training and experience and the facts set forth herein, I submit there is probable cause to believe that Manlapaz and others known and unknown to the investigation have committed violations of 26 USC § 7206(2), conspiracy to defraud the United States, in violation of 18 USC §§ 371 and 1349, mail fraud, in violation of 18 USC § 1341, wire fraud, in violation of 18 USC § 1343, identity theft, in violation of 18 USC § 1028(a)(7), and money laundering, in violation of 18 USC §§ 1956, 1957.

49. Based on my training and experience and the facts set forth above, I submit that there is also probable cause to believe that evidence, contraband, and fruits of these offenses exist on computer systems in the control of Facebook. I therefore respectfully request that the Court issue a warrant requiring **Facebook** to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment B for the accounts identified in Attachment A.



Michael J. Wheeler
Special Agent, IRS-CI

Subscribed and sworn to before me this 26th day of October, 2017.



John F. Anderson
United States Magistrate Judge
Honorable John F. Anderson
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF)
INFORMATION ASSOCIATED WITH)
FACEBOOK USER IDs:)

Case No. 17-SW-~~709~~ 708

“Ben.Manlapaz.JBMFinancialGroup”, and)
“100008768172560”.)

UNDER SEAL

)
STORED AT PREMISES CONTROLLED)
BY FACEBOOK INC.)

ATTACHMENT A
Places to Be Searched

This warrant applies to any and all information associated with the Facebook IDs
“Ben.Manlapaz.JBMFinancialGroup” and “100008768172560,” that are stored at a premises
owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in
Menlo Park, California.

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF)
INFORMATION ASSOCIATED WITH)
FACEBOOK USER IDs:)

Case No. 17-SW-~~709~~ 708

“Ben.Manlapaz.JBMFinancialGroup”, and)
“100008768172560”.)

UNDER SEAL

STORED AT PREMISES CONTROLLED)
BY FACEBOOK INC.)

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by FACEBOOK, Inc. (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A for the period of 2008 to present:

- (a) All activity logs for the account and all other documents showing the user’s posts and other Facebook activities;
- (b) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;
- (c) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which

- the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;
- (d) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;
 - (e) All "check ins" and other location information;
 - (f) All IP logs, including all records of the IP addresses that logged into the account;
 - (g) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";
 - (h) All information about the Facebook pages that the account is or was a "fan" of;
 - (i) All past and present lists of friends created by the account;
 - (j) All records of Facebook searches performed by the account;
 - (k) All information about the user's access and use of Facebook Marketplace;
 - (l) The types of service utilized by the user;
 - (m) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
 - (n) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

- (o) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.
- (p) The files, contents and metadata associated with the accounts related to Facebook services such as Facebook Likes, Facebook search history, Facebook bookmarks, Facebook drive files, Facebook purchases, Facebook Sites, Facebook notifications, Facebook uploads and activity (including but not limited to the user's profile, posts, chats, messages and emails, comments), Facebook followers.
- (q) All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number), screen names, Facebook security questions and answers, contact email addresses, websites and other personal identifiers;
- (r) Records or information (cookie data), to include unique identifying information, of all devices that have accessed target accounts

II. Information to be Seized by the Government

A. All information described in Section I above, including but not limited to correspondence, records, documents, photographs, videos, electronic mail, chat logs, and electronic messages, that constitutes evidence, contraband, and fruits of violations of the

preparation of false and fraudulent tax returns (26 U.S.C. § 7206(2)), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), conspiracy to defraud the United States (18 U.S.C. §§ 371, 1349), money laundering (18 U.S.C. §§ 1956, 1957), and identity theft (18 U.S.C. § 1028(a)(7)), including, for each account or identifier listed on Attachment A, information pertaining to the following matters for the period of 2008 through present:

1. Any records, documents, communications or other materials related to the preparation of federal income tax returns or state tax returns;
2. Any records, documents, communications or other materials related to communications with the U.S. Internal Revenue Service or state tax authorities;
3. Any records, documents, communications or other materials related to advertising the services offered by JBM, including but limited to those related to tax preparation, ITINs, or responding to IRS letters/audits;
4. Any records, documents, communications or other materials related to the identities, roles, and relationships of employees in JBM, including who had a management and/or supervisory role;
5. Any records, documents, communications or other materials related to the IRS criminal investigation, including the search in 2013;
6. Any records, documents, communications or other materials related to the training, certifications or qualifications of Ben Manlapaz or others employees of JBM to prepare tax returns;
7. Any records, documents, communications or other materials related to identifying clients of JBM;

8. Any records, documents, communications or other materials related to the disposition of proceeds earned by Ben Manlapaz and/or JBM, including the manner and means for paying employees in the Philippines;
9. Any records, documents, communications or other materials related to the use of cash or the sending of JBM proceeds outside of the United States;
10. Any records, documents, communications or other materials related to books and records of JBM, including any client lists;
11. Any records, documents, communications or other materials related to the JBM office in the Philippines and its role in preparing materials submitted to the IRS or state tax authorities;
12. Any records, documents, communications or other evidence showing who used, owned, or controlled the accounts or identifiers listed on Attachment A;
13. Any records, documents, communications or other evidence of the times the accounts or identifiers listed on Attachment A were used, updated or revised;
14. Any records, documents, communications or other evidence of passwords or encryption keys and other access information that may be necessary to access the accounts or identifiers listed on Attachment A and other associated accounts.